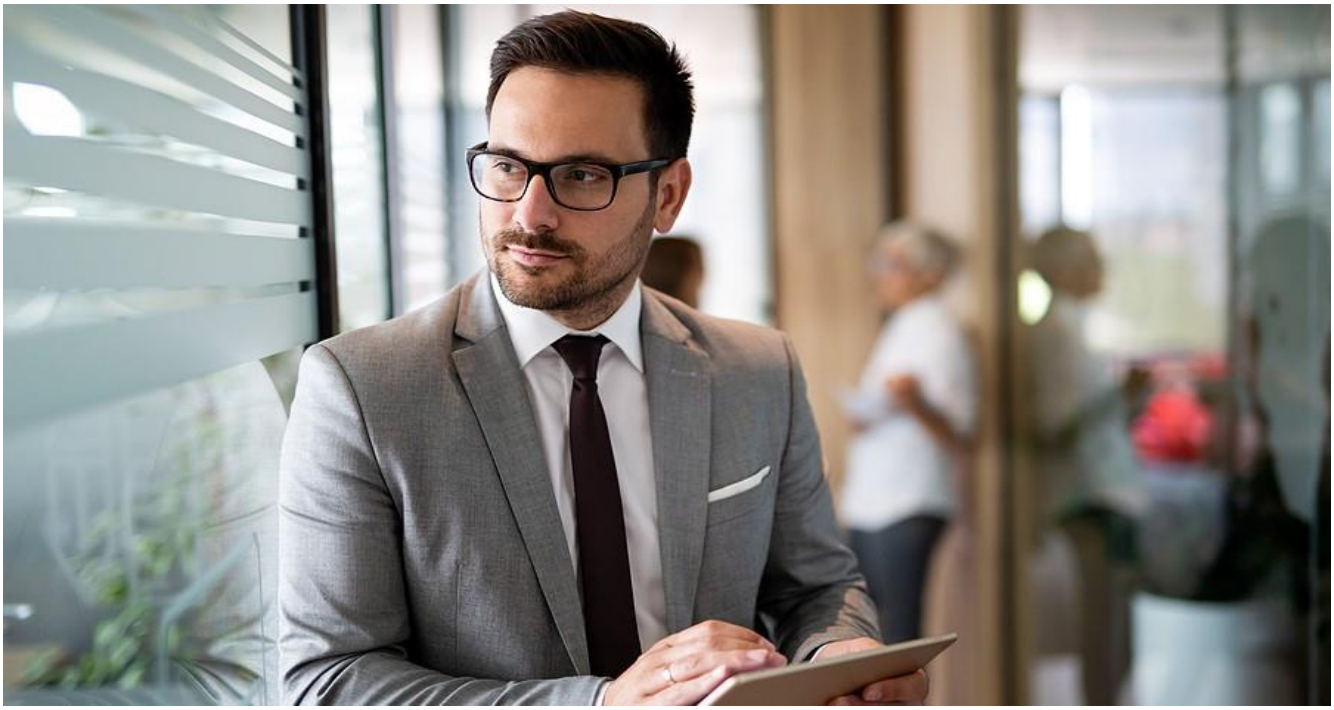
4 Cyber Security Risk Factors Companies Must Address in 2024



As businesses approach the new year, they must tackle cyber security risk factors that could leave them exposed to attack. Emerging cyber threats such as those posed by AI require organizations to find and fix gaps in their security strategies. And common security weak spots such as IoT devices, supply chain vulnerabilities, and human factors also demand attention.

IoT Creates Open Doors for Hackers

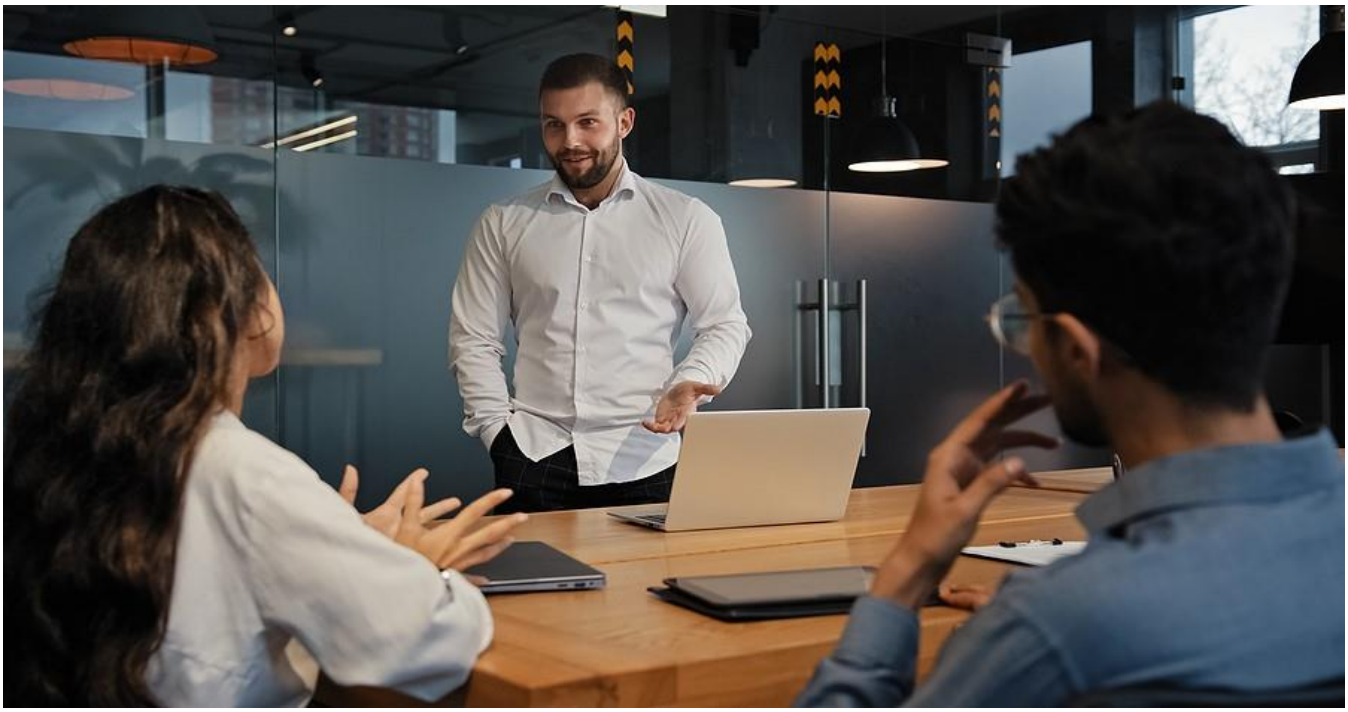
The IoT refers to the network of devices embedded with sensors and software to collect and exchange data. IoT devices can include items such as security cameras, printers, and even smart appliances like coffee makers.

Many of these devices seem harmless and of little value to criminals. In the case of security cameras, they may even play a role in providing security. However, because they connect to the network and can be compromised easily, they present a favorite target for hackers. Not only do they provide an entry point into the network, but they can be used to create botnets.

These botnets refer to networks of compromised devices controlled by a central command and control server. Hackers use them to launch cyber attacks such as denial of service (DoS), spamming, or credential stuffing. And they can create these botnets out of any device connected to the internet.

Because they are not typically designed with security in mind, IoT devices pose a serious security hazard. In the first place they often come with weak or default passwords that many users do not

change. They also frequently lack proper encryption and security protocols. And because they fly under the radar, many users do not install security updates.



Supply Chain as a Steppingstone

The supply chain presents another favorite target for attackers. While larger organizations tend to invest in robust cyber security, SMBs often lack the resources and expertise to strengthen security. When hackers compromise a small vendor organization, they can then use that access to infiltrate larger, more lucrative targets.

In fact, a 2023 study by Cybersource reported that SMBs accounted for 28 percent of cyberattack victims. This underscores the need for larger enterprises to rigorously monitor the security postures of their third-party vendors and SMB partners.

Additionally, to counter both supply chain and IoT threats, organizations should adopt a zero-trust architecture. This means that the system verifies the identity and context of every user, device, and request before granting access. It also involves enforcing strong encryption and applying security policies based on the principle of least privilege.

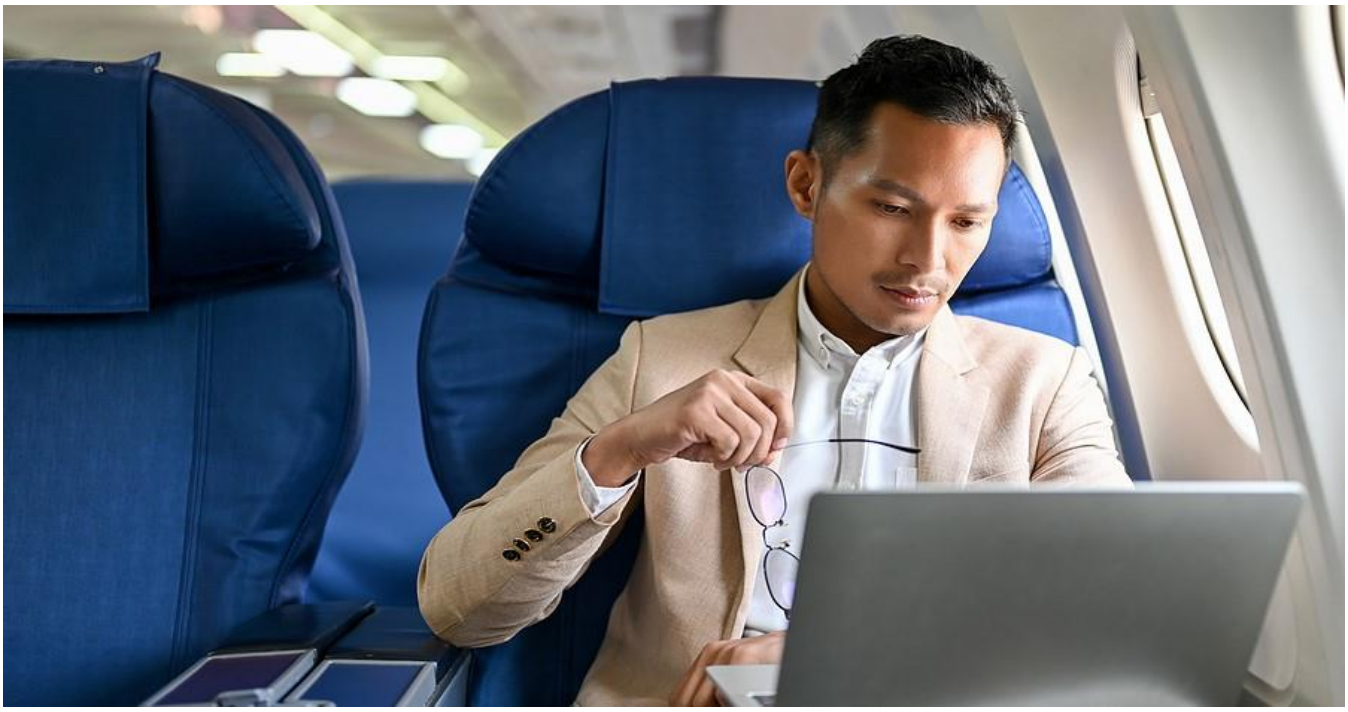
Humans Present Challenges

Even with increasingly sophisticated security tools, humans continue to present a significant risk factor. Every time employees use weak passwords, click on phishing links, or bypass security controls, they create hazards.

To address this risk, organizations should adopt a human-centric security design. This approach considers the human factors that influence security behavior. It involves adopting security controls that employees can easily understand and use. And it includes incentives and timely feedback to encourage employees to follow security best practices.

For example, human-centric security design might involve using biometric authentication instead of passwords. It could also include gamifying security awareness training or offering context-sensitive reminders.

In addition to security awareness training, security teams should implement technical measures to prevent or reduce the impact of phishing. These include implementing strong email security solutions, encrypting sensitive data, and conducting regular backups.



Cyber Security Skills Gap

Implementing effective cyber security requires a diverse set of skills and competencies. However, hiring qualified security professionals can prove difficult and expensive. In fact, CompTIA estimates that the cyber security workforce gap has grown to nearly 3 million positions.

To close this gap, organizations have a couple of options. They can invest the budget and time required to develop their own cyber security talent pipeline. Or they can leverage external security partners to enhance security operations, thus gaining access to top-level expertise and tools.

Conquer Cyber Security Risk Factors with Comprehensive Strategy

Today's sophisticated cyber threats necessitate a holistic and proactive approach to cyber security. Rather than relying on outdated defenses or reacting to incidents after they occur, businesses should adopt a comprehensive and integrated cyber security strategy.

The cyber security experts at eMazzanti Technologies can help. Beginning with a cyber security assessment, they work with organizations to customize security strategies to business needs and budgetary constraints.